AO 106 (Rev. 06/09) Application for a Search Warrant

FILED

APR 12 2019

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
INFORMATION ASSOCIATED WITH SNAPCHAT ACCOUNT "KURTOLSEN" THAT IS STORED AT A PREMISES CONTROLLED BY SNAP INC.

Case No. 19-mj-82-PJC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A" of description of property to be searched.

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B" of property to be seized.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
See Attachment "C."	

The application is based on these facts:

See Attached Affidavit by Evan D. Held, SA/FBI

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 180 days (give exact ending date if more than 30 days: Oct 12, 2019) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

EVAN D. HELD, SA/FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 4/12/2019

Judge's signature

City and state: Tulsa, OK

US Magistrate Paul J. Cleary
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH SNAPCHAT ACCOUNT "KURTOLSEN" THAT IS STORED AT A PREMISES CONTROLLED BY SNAP INC.	Case No. 19-mj-82-PJC **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Evan D. Held, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Snapchat account stored at premises owned, maintained, controlled, or operated by the social media company Snap Inc. Snap Inc. makes the mobile application Snapchat and is headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Snap Inc. to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Snapchat account identified in Attachment A.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI), and have been so employed since my graduation from the FBI's New Agent Training in Quantico, Virginia, on February 15, 2013. As a Special Agent, my duties include, but are not limited to, investigating violations of federal criminal law and threats to national security. My investigations into violations of federal criminal law include, but are not limited to, computer intrusions, threatening

communications, and counterterrorism. I am currently assigned to the FBI's Oklahoma City Field Office, Tulsa Resident Agency.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

4. Based on my training, research, experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of:

- Title 18, United States Code, Section 1030(a)(2)(c) – Fraud and related activity in connection with computers;
- Title 18, United States Code, Section 1028(a)(7) – Fraud and related activity in connection with identification documents, authentication features, and information.

have been committed, and that evidence of these crimes are located in the place described in Attachment A. For this reason, I request to seize all items listed in Attachment B as evidence or instrumentalities of the crime.

BACKGROUND ON SNAPCHAT

5. Snapchat is a free mobile application made by Snap Inc. and available through the Apple App Store and Google Play Store. The Snapchat app provides users a way to share moments with photos, videos, and chats.

6. "Snaps" are photos or videos taken using the camera on an individual's mobile device through the Snapchat app, and may be shared directly with the user's friends, or in a story (explained further below), or chat.

7. A Snapchat user can add Snaps to their "story." A story is a collection of Snaps displayed in chronological order. Users can manage their privacy settings so that their story can be viewed by all Snapchatters, their friends, or a custom audience. A user can also submit their Snaps to Snapchat's crowd-sourced service "Our Story," which enables their Snaps to be viewed by all Snapchatters in Search and Snap Map.

8. "Memories" is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. Content saved in Memories is backed up by Snap and may remain in Memories until deleted by the user. Users may encrypt their content in Memories, in which case the content is not accessible to Snap Inc. and cannot be decrypted by Snap Inc.

9. A user can type messages, send Snaps, audio notes, and video notes to friends within the Snapchat app using the Chat feature. Snapchat's servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user's chat settings.

10. If a Snapchat user has device-level location services turned on and has opted into location services on Snapchat, Snap Inc. will collect location data at various points during the user's use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

11. A Snapchat username is a unique identifier associated with a specific Snapchat account, and it cannot be changed by the user.

12. Basic subscriber information is collected when a user creates a new Snapchat account, alters information at a later date, or otherwise interacts with the Snapchat app. The basic subscriber information entered by a user in creating an account is maintained as long as the user has not edited the information or removed the information from the account.

13. In light of the foregoing, Snap constitutes a provider of an "electronic communication service" within the meaning of 18 U.S.C. § ~~3123~~ 2510(15) EDK.

PROBABLE CAUSE

14. Based on Affiant's training, research, and experience, social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. E-mail and social media providers commonly offer options to reset the password for an account when it has been lost or forgotten. Recovery options often include sending a message with a security code to a known phone number or an e-mail address associated with the account. These recovery phone numbers and e-mail addresses are often established by the account owner upon registration with the service, but can usually be established at a later time. If an unauthorized user is able to obtain the security code through the use of social engineering, the unauthorized user may be able to log into an account and change the account's password.

VICTIM #1

15. Victim #1, a 19 year old female, who resided within the jurisdiction of the Northern District of Oklahoma, was interviewed by Affiant and FBI Task Force Officer (TFO) Lissa J. Kennedy on July 9, 2018. During the interview, Victim #1 (hereinafter referred to as VI#1) advised that on March 16, 2018 at approximately 4:04PM, she received a text message on her cellular phone from 918-322-7874 purporting to be from "Ashley." VI#1 did have a friend named Ashley,

but did not recognize the phone number from which the text originated. The user of phone number 918-322-7874 later identified themselves as "Territory."

16. On July 10, 2018, VI#1 provided screenshots of text messages exchanged between her phone number and a number used by Territory. Relevant text messages exchanged between VI#1 and Territory have been transcribed below:

> ***Territory:*** *Hi sorry to bother you but I put the wrong number on my yahoo account and I can't login without the code please help me*
> ***Territory:*** *My name is Ashley please help me I just need the code*
> ***VI#1:*** *XXFFGFTX is Your Yahoo Account Key*
> ***Territory:*** *Thanks let me try it*
> ***Territory:*** *Let me send it again sorry*
> ***Territory:*** *Okay can you send me the new code please*
> ***Territory:*** *Last code*
> ...
> ***VI#1:*** *You're not real and you hacked my Facebook. What the fuck.*
> ***Territory:*** *What do you mean?!*
> ***Territory:*** *Lol get hacked*
> ***Territory:*** *Now i am about to destroy u*
> ***VI#1:*** *What did you do.*
> ***Territory:*** *Do something for me and I'll give everything back*
> ***VI#1:*** *What's that.*
> ***Territory:*** *Put my name on your boobs*
> ***Territory:*** *And take a picture and send*
> ***VI#1:*** *And what's ur name?*
> ***Territory:*** *My hacking name Territory*
> ...
> ***Territory:*** *Last chance*
> ***Territory:*** *Take it or I hack everything*
> ***VI#1:*** *Why are you doing this ???? Like why?*
> ***Territory:*** *Hurry up*
> ***Territory:*** *Last chance*
> ***Territory:*** *Before i hack your PayPal and credit cards*
> ***VI#1:*** *What exactly do you want seriously*
> ***Territory:*** *I want you to put my name on your boobs and take a picture and send me it*
> ***Territory:*** *Simple as that*

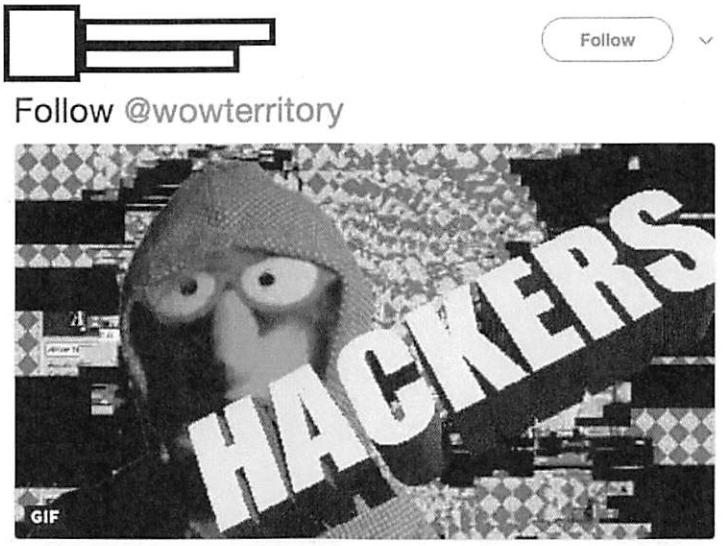
VI#1: *Seriously that's it?*
VI#1: *And then what!? Where does that go*
Territory: *Yes*
Territory: *And I'll stop*
Territory: .
VI#1: *Just for you to keep or what*
Territory: *Yes no one is gonna see it*

17. VI#1 refused Territory's demand for the photograph.

18. During subsequent telephonic interviews with Affiant, VI#1 explained how she located the webpage of Twitter username @wowterritory. VI#1 was contacted by a female friend hereinafter referred to as "N.G." According to VI#1, Territory previously tried to hack N.G. N.G. told VI#1 to look at the Twitter username @wowterritory. After creating a new Twitter account using a fake name, VI#1 looked up Twitter username @wowterritory and saw a Tweet with her bank card information. VI#1 advised she cancelled the bank card and did not suffer any financial loss.

19. During the July 9, 2018, interview, VI#1 said she was scared for her safety due to the Tweets she observed on Territory's Twitter page @wowterritory. VI#1 recalled a Tweet on Twitter username @wowterritory's page which said the Parkland shooting victims deserved it. VI#1 observed other Tweets referencing ISIS and support for school shootings.

20. On July 12, 2018, Affiant accessed VI#1's Twitter page. Affiant observed and captured the following Tweet posted on or about March 16, 2018:



21. The above screenshot depicts a Tweet containing an animated digital photograph which automatically replays itself. In observing the image, Affiant observed the animated digital photograph to state: "oh no, HACKERS in the MAINFRAME!"

22. Affiant noted the date the Tweet was created was March 16, 2018. This was the same day VI#1 was first contacted via text message by Territory.

23. In a telephonic interview with Affiant and FBI SA Stephen Carnevale on September 4, 2018, VI#1 advised she did not author the Tweet.

DOXING OF "TERRITORY"

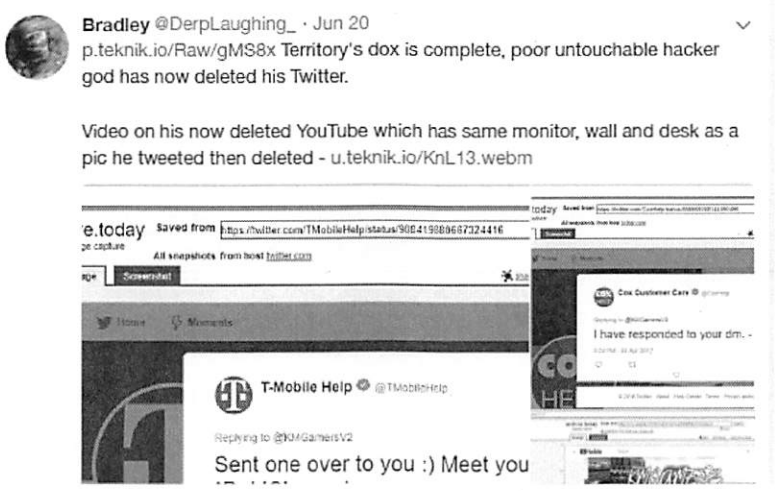
24. Based on Affiant's training, research, and experience, "doxing" can be a practice among hackers in which one hacker will publicly release the identifying information of another hacker's online persona. Based on Affiant's training, research, and experience, "doxing" may be carried out for various reasons, including, but not limited to: shaming the party in question, righting perceived wrongs, and/or to intimidate.

25. On July 2, 2018, Affiant conducted open source research of terms relevant to the investigation to include, but not limited to, "Territory" and "hacker." Affiant located the webpage of Twitter username @DerpLaughing_ (https://www.twitter.com/DerpLaughing_/) which contained links to a dox of Territory. As detailed below, the author of the dox exposed Territory's identity in response to his illicit online activities.

26. Two Tweets observed on @DerpLaughing_'s Twitter page are depicted below:

Tweet #1:

Tweet #2:



27. Based on Affiant's training, research, and experience, Affiant interprets the Tweets depicted above as @DerpLaughing_ mocking, humiliating, and ridiculing Territory.

28. Affiant noted the Tweets depicted above contained links to Ghostbin and Teknik.io. Based on your Affiant's training, research, and experience, Ghostbin and Tecknik.io provide the ability to post text, which can become publicly accessible on the Internet. Affiant visited webpage

http://ghostbin.com/paste/7rkk9 and reviewed the content of the dox. The introduction portion of the dox states, in part, the following:

Excerpt #1:

> It has come to our attention that a skid by the name of "territory" has been making his rounds on the internet lately.... mostly by pretending to be Elliot from Mr. Robot and extorting teenaged girls for "booby pictures". Although brainless wastes of oxygen like him can be found simply by looking up "how to install kali linux", "territory" is of particular interest to us because of his obsession with (a) female attention and (b) his subsequent sperglord rage sessions when women on the internet inevitably deny his advances. "Territory" has been doxing, extorting and sexually harassing women since 2015. the hacker at pen0 will NOT tolerate such a blatant challenge to our position as the most autistic demographic in the universe.
>
> Territory has referred to himself as "an undoxable hacker god" multiple times. Maybe it's his mantra that he learned in his Socialization and Making Friends class in Special Ed, we don't know. As you, the reader, will find out shortly, the only thing Territory holds godlike status in is a supreme lack of self-awareness and general intelligence. Karlos is probably only one bad fall away from being a total Michael Schumacher, and we here at public-enemy-number-0 are here to ensure that he never rubs his last 2 brain cells again.

29. The dox also contained the following statement which Affiant interpreted as a possible motivation for its publication: "I'm sure that the victims of your extortion campaign will appreciate this informat[ion] and I can already bet you that it's on the way to the FBI."

30. The dox also claimed to identify Territory as "Karlos Masood (Eshaq) Saka" at address "1347 PEPPER DR, SPC 8, EL CAJON, CA[.]"

31. Affiant is unaware of how the information in the dox was obtained.

32. Affiant obtained California Department of Motor Vehicles records from another FBI employee which confirmed there was a person by the name of Karlos Masood Saka, date of birth January 1, 2000, at a mailing address of 1347 Pepper Drive, 8, El Cajon, California.

33. Notably, excerpt #2 from the dox, as depicted below, appears to show an exchange of text messages between phone number 918-322-7874 and an unspecified number. Affiant noted phone number 918-322-7874 was the same number reported by VI#1. Moreover, the content of

the messages depicted in Excerpt #2 were almost identical to the text messages provided to the FBI by VI#1.

Excerpt #2:

[TEXTS FROM NUMBER +1(918)3227874]
Lol get hacked
Now i am about to destroy you
[reply] what did you do.
Do something for me and i'll give everything back
Put my name on ur boobs
And take a picture and send <---------- HAHAHAHAH

[reply] And whats ur name?
My hacking name Territory
:smiley emoji:
Last chance
Take it or i hack everything
[reply] Why are you doing this???? Like why?
Hurry up
last chance
Before i hack your PayPal and credit cards

As we can clearly see from these text logs, Territory is an unfearing psychopath who gives ZER0 FUCKS and will use his 1337 "hello i forgot my password" hacking skills to lay waste to ANY teenage mexican 15 year old that dares glance at his cold, dead, intelligent eyes.

okay LOL
Deleteing this app
Cya thanks for your stuff and credit card
Gave u a chance
:laughing emoji:
It's called vpn
:heart emoji:
Which changes your address and ip
your[sic] a fucking retard

34. Based on Affiant's training, research, and experience, the term "l337" as used above in Excerpt #2 is a term used on Internet forums and messages boards, which means "leet," or "elite." Affiant interprets the author's use of the phrase "1337 "hello i forgot my password" hacking skills" to further mock and ridicule Territory by satirically using the phrase.

35. In addition to the three excerpts above, the dox Tweeted by DerpLaughing_ included a list of aliases used by Territory which included, but was not limited to: DdosMyWifi, imterritory, MaskedSpooky, itst3rritory and wowterritory.

SAN DIEGO COUNTY SHERIFF'S DEPARTMENT

36. The N-Dex system is an unclassified national information sharing system that enables criminal justice agencies to search, link, analyze, and share local, state, tribal, and federal records. Affiant located San Diego County Sheriff's Department (SDSD) report number 17116533.1 listing Karlos M Saka (hereinafter referred to as Saka) as a subject. On August 21, 2018, FBI Task Force Officer (TFO) Todd A. Richards provided Affiant with a copy of the report.

37. The investigation conducted by SDSD identified five (5) victims who reported their social media accounts were hacked and demanded nude photographs for return of the accounts. Saka was interviewed during the course of SDSD's investigation. After being provided his Miranda rights, Saka advised he wanted to speak to law enforcement officers without the presence of his attorney. In the report, the interviewing officer provided a synopsis of the interview. Excerpts of the synopsis relevant to this investigation are depicted below:

> *Karlos stated he was called into [Vice Principal] Battle's office because he was involved in "hacking" girls' accounts. Karlos stated Diego, Angelo and himself were breaking into girls social media accounts to find photographs of them.*
>
> *Karlos stated he requests a password change for the email account. He puts in the individual girl's cell phone and then sends them a fake text through an application called "FreeText." Karlos states he accidently used their number and requests they send the verification code to him. If the victim's sent the code, Karlos then changed their account to his password and changes the rest of their social media accounts.*
>
> *Karlos admitted to getting into the girls' iCloud to look for nude photographs but stated he never asked for any.*
>
> *[...]*
>
> *Karlos stated they call themselves "MaskedSpooky[.]"*

38. Affiant noted the method of hacking Saka admitted to using in the interview with SDSD was the same method used to access VI#1's accounts.

RIVERSIDE COUNTY SHERIFF'S DEPARTMENT

39. Saka was arrested by the Riverside County, California Sheriff's Department (RCSD) on September 19, 2018 on charges stemming from his suspected involvement in extortion and computer hacking. RCSD Master Investigator Robert M. Cornett provided Affiant with an interview summary. Affiant reviewed the interview summary, and relevant portions of the interview are detailed below.

40. After being advised of his Miranda Rights, Saka agreed to speak to law enforcement officers. Investigators explained to Saka that they were investigating an incident similar to what he was arrested for in San Diego, California in February 2017. When asked if he knew why investigators were speaking with him, Saka said no. Investigators then showed Saka a photo of a victim's breasts with "Territory" written on it. Investigators then asked Saka if he understood why investigators were talking with him, and Saka shook his head yes.

41. Investigators then asked Saka how he did this, and Saka said he would get the person's phone number and text them saying he was "Ashley." Saka would then explain he accidentally put the victim's phone number into "Ashley's" account and an authorization code was sent to the victim's phone number. Saka, posing as "Ashley," asked for the authorization code. If Saka obtained the code, then Saka can log into the account he is hacking. Saka said he would use a "fake text app" to text the victim.

KURT OLSEN – VICTIM

42. Kurt Olsen, a 23 year old male, who resided in Broken Arrow, Oklahoma, was interviewed by Affiant and Task Force Officer William H. Jenkins on December 4, 2018. During the interview, Olsen advised his Snapchat account "kurtolsen" was hacked in approximately November 2017.

43. An unknown individual threatened to hack Olsen's girlfriend if she did not send nude photographs. Olsen was "pretty sure" the unknown individual used a Snapchat account with a name similar to "T3rritory." Olsen exchanged messages with the unknown individual in an attempt to defend his girlfriend. Approximately two weeks after exchanging messages with the unknown individual, Olsen was unable to log-in to his Snapchat account and learned the e-mail address associated with the account had been changed.

44. In approximately November 2017, Olsen's friends contacted him to inquire whether his Snapchat account had been hacked. Olsen's friends continued to ask about his former Snapchat account until approximately January 2018. Olsen reported his hacked account to Snapchat approximately three (3) or four (4) times, but the page was not taken down.

45. In approximately November 2018, Olsen learned of a post on Twitter indicating his hacked account was possibly being used again.

VICTIM #2

46. Victim #2, a 21 year old female, who resides within the jurisdiction of the Northern District of Oklahoma, was interviewed by TFO Christopher J. Claramunt and TFO William H. Jenkins on January 11, 2019. Victim #2 (hereinafter referred to as VI#2), added Kurt Olsen, an old classmate of Broken Arrow High school, to her Snapchat account. VI#2 began exchanging messages with the individual she believed to be Olsen. The individual using Olsen's account later requested VI#2 to send "boodie pics" and "nudes." VI#2 became uncomfortable and defriended the Snapchat account she associated with Olsen.

47. In or around November 2018, VI#2 and Olsen began spending time together socially and added Olsen back on Snapchat. On December 23, 2018, VI#2 received a Snapchat

message from Olsen's account of a full nude photograph of Olsen. VI#2 did not discuss the image with Olsen.

48. On December 31, 2018, VI#2 received a message from Olsen on Snapchat that requested she send a Yahoo verification code that had been sent to her. VI#2 sent the code to Olsen's Snapchat account, not realizing the code was for her own Yahoo account.

49. VI#2 checked her Snapchat account after sending the code and discovered she was locked out of her account. Later, VI#2 learned the e-mail address to her Snapchat and Instagram accounts had been changed. VI#2 was able to recover access to her Yahoo e-mail account, Instagram account, and Snapchat account.

50. A request for preservation of records for account "kurtolsen" was submitted to Snap Inc. on January 2, 2019. An extension request was submitted on February 26, 2019.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

51. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Snap Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

52. Based on Affiant's training, research, experience, and the interviews conducted by the FBI, Affiant believes records and other information in the possession of Snap Inc. will contain evidence of crimes to include violations of Title 18, United States Code Sections 1030(a)(2)(c)

and 1028(a)(7) and evidence regarding how the Snapchat account was used as an instrumentality of a crime.

53. Based on the forgoing, I request that the Court issue the proposed search warrant.

54. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

55. Because the warrant will be served on Snap Inc., which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

56. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

57. Affiant requests to be allowed to share this affidavit and the information obtained from this search (to include copies of digital media) with any government agency, to include state and local agencies, investigating, or aiding in the investigation of, this case or related matters.

REQUEST FOR SEALING

58. Affiant further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all

of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Evan D. Held
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on the 12th day of April, 2019.

PAUL J. CLEARY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Snapchat account "kurtolsen" (hereinafter the "Target Account"), which is stored at the premises owned, maintained, controlled, and/or operated by Snap Inc., a company headquartered in Santa Monica, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Snap Inc. (hereinafter "the Provider"):

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any messages, records, files, logs, photographs, videos or other information that has been deleted but is still available to the Provider, or has been confirmed preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account listed in Attachment A: (the "Target Accounts"):

(a) All stored communications and other files in Snap's possession (including account access information, event histories including dates and times, connection dates, times and locations, connection IP information, message content, graphics files, attachments, etc., further detailed below), whether physical, stored on electronic media, or temporarily extant on any computer or server, reflecting communications to or from the Target Accounts;

(b) All subscriber information, including: Snapchat username vanity names; email addresses; phone numbers; full name; physical address; and other identifiers;

(c) All information pertaining to creation of the account, including: Date and time of creation; IP address used to create the account; all subscriber information provided at the time the account was created;

(d) Timestamp and IP address of all account logins and logouts;

(e) Logs of all messages and all files that have been created and Snaps sent/or accessed via the Target Accounts or that are controlled by user accounts associated with the Target Accounts;

(f) The account name, vanity name, identifiers and all available subscriber information for any other Snapchat account(s) associated with the Target Accounts;

(g) All connection logs and records of user message activity, including all meta-data;

i. Transmitter/Sender identifier (i.e. addresses and/or IP address);

ii. Connection date and time;

iii. Method of connection (telnet, ftp, http);

iv. Data transfer volume;

v. User name associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;

vi. Account subscriber identification records;

vii. Other user accounts associated with, referenced in or accessed by the Target Accounts;

viii. Address books, contact lists and "my friends";

ix. Records of files or system attributes accessed, modified, or added by the user;

x. All records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with the Target Accounts, including, without limitation, subscriber names, user names, screen names or other identities, addresses, residential addresses, business addresses, and other contact information, telephone numbers or other subscriber number or identifier number, billing records, information about the messages and Snaps and all information length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form. Such records and other

evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content associated with or relating to postings, communications and any other activities to or through the Target Accounts, whether such records or other evidence are in electronic or other form;

(h) All records pertaining to communications between Snapchat and the users of the Target Accounts regarding the user or the user's Snapchat account, including contacts with support services and records of actions taken;

(i) The content of all messages and Snaps sent, received, and saved, stored, or preserved.

II. Information to be seized by the government

(a) All information described in Section I that constitutes fruits, evidence, and instrumentalities of violations of:

i. Title 18, United States Code, Section 1030(a)(2)(c) – Fraud and related activity in connection with computers;

ii. Title 18, United States Code, Section 1028(a)(7) – Fraud and related activity in connection with identification documents, authentication features, and information.

(b) Records, information, and items relating to the violations of the statutes described above including:

i. Evidence of the identity of the user, owner, or individual(s) who control the Target Accounts;

ii. Evidence indicating the Target Account user's knowledge and/or intent as it relates to the above violations;

iii. Evidence indicating the times, geographic locations, and electronic devices from which the Target Accounts were accessed and used to determine the chronological and geographic context of the Target Account access, use and events relating to the violations under investigation and to the owner(s) of the Target Accounts;

iv. Passwords, encryption keys, recovery e-mail accounts, contact information, security questions, phone numbers, and other access information used to access the Target Accounts;

(c) As used above, the terms "documents," and "communications," refers to all content regardless of whether it is in the form of pictures, videos, audio records, text communications, or other medium, and whether in draft or completed form and whether sent or received;

(d) As used above, the terms "records" and "information" includes all forms of data stored by the Provider including IP addresses, toll records, and account identifying information.

(e) Evidence indicating how and when the Snapchat account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crimes under investigation to the Snapchat account owner;

(f) Evidence indicating the Snapchat account owner's state of mind as it relates to the crime under investigation;

(g) Evidence indicating the geographic location of the cellular device at times relevant to the investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

(i) The identity of the person(s) who sent and/or received communications from the device.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Snap Inc., and my official title is _____. I am a custodian of records for Snap Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Snap Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Snap Inc.; and

c. such records were made by Snap Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature